CLAIMS

1. A method of authorising a key or lock device, comprising the following steps:

- creating a first user device having an electronic circuitry,

- creating a first system device having an electronic circuitry and being used in a first level of a lock system,

- storing a first encryption key in said first user device and said first system device,

- carrying out an authentication process between said first user device and said first system device using said first encryption key, and

- in case said authentication process was successful, carrying out a software operation by said first system device, by which software operation said first encryption key stored in said first user device is replaced by a second encryption key,

- wherein said second encryption key is stored in second system devices and user devices used in a second level of said lock system, thereby making said first user device operable with said second system and user devices.

2. The method according to claim 1, wherein, during the step of replacing said first encryption key stored in said first user device, said second

encryption key is supplied by said first system device.

3. The method according to claim 1, wherein, during the step of replacing said first encryption key stored in said first user device, said second encryption key is supplied by a computer.

4. The method according to claim 3, comprising the additional step of supplying said second encryption key to said computer through a network including local networks and public telephone networks.

5. The method according to claim 1, wherein said first system device is a system key of a master key system.

6. The method according to claim 1, wherein said first user device is a user key of a master key system.

7. The method according to claim 1, wherein said first user device is a lock of a master key system.

8. The method according to claim 1, wherein said electronic encryption keys are unreadable from outside said electronic circuitry.

9. An electromechanical key and lock device, comprising:

- an electronic circuitry having an electronic memory adapted for storing an electronic code, said electronic code uniquely identifying the device and comprising a first electronic encryption key,

- wherein said first encryption key being adapted to be replaced by a second encryption key by means of an authenticated software operation carried out by a first system device having said first encryption key and being used in a first level of a lock system, and

- said second encryption key is stored in system and user devices used in a second level of said lock system, thereby making said first user device operable with said second system and user devices.

10. The device according to claim 9, wherein said first system device is a key having a programmable electronic circuitry.

11. The device according to claim 9, wherein said electronic encryption keys are unreadable from outside said electronic circuitry.

12. A key and lock system comprising:

- a plurality of user devices comprising:

  - a plurality of user keys having an electronic circuitry comprising an electronic memory adapted for storing a variable electronic encryption key, and

  - a plurality of locks having an electronic circuitry comprising an electronic memory adapted for storing a variable electronic encryption key,

- wherein a user key and a lock are operable only if there are stored identical encryption keys in said user key and the lock,

- at least one system device having an electronic circuitry comprising an electronic memory adapted for storing a permanent electronic encryption key, and

- a computer program software adapted to change the variable electronic encryption key of a user device from a first to a second encryption key as a result of a successful authentication process carried out between

  - a lock or user key having a stored variable electronic encryption key, and

  - a system device having an identical encryption key as said lock or user key.